Claims

[c1] What is claimed is:

1.A method of preventing firmware from being pirated, the firmware containing executable code for an electronic device, the method comprising:

ciphering executable firmware code into ciphered firmware code;

storing the ciphered firmware code in a nonvolatile memory of the electronic device;

storing a decipher key in a decrypting circuit of the electronic device;

deciphering the ciphered firmware code with the decrypting circuit of the electronic device to decrypt the executable firmware code;

storing the executable firmware code in a volatile memory of the electronic device; and

executing the executable firmware code stored in the volatile memory for operating the electronic device.

[c2] 2.The method of claim 1 wherein software installed on a host computer ciphers the executable firmware code into the ciphered firmware code.

[c3] 3.The method of claim 2 wherein the software installed

on the host computer transmits the ciphered firmware code to a firmware refresh circuit of the electronic device and the firmware refresh circuit stores the ciphered firmware code in the nonvolatile memory of the electronic device.

[c4] 4.The method of claim 2 wherein the software installed on the host computer transmits the ciphered firmware code to a firmware burner, the firmware burner is connected to the electronic device, and the firmware burner stores the ciphered firmware code in the nonvolatile memory of the electronic device.

[c5] 5.The method of claim 1 wherein the nonvolatile memory is flash memory.

[c6] 6.The method of claim 1 wherein the volatile memory is dynamic random access memory (DRAM).

[c7] 7.The method of claim 1 wherein the electronic device is an optical disk drive.

[c8] 8.The method of claim 1 wherein the electronic device is a hard drive.

[c9] 9.The method of claim 1 wherein the electronic device is a computer and the executable firmware code is code in a basic input output system (BIOS) of the computer.